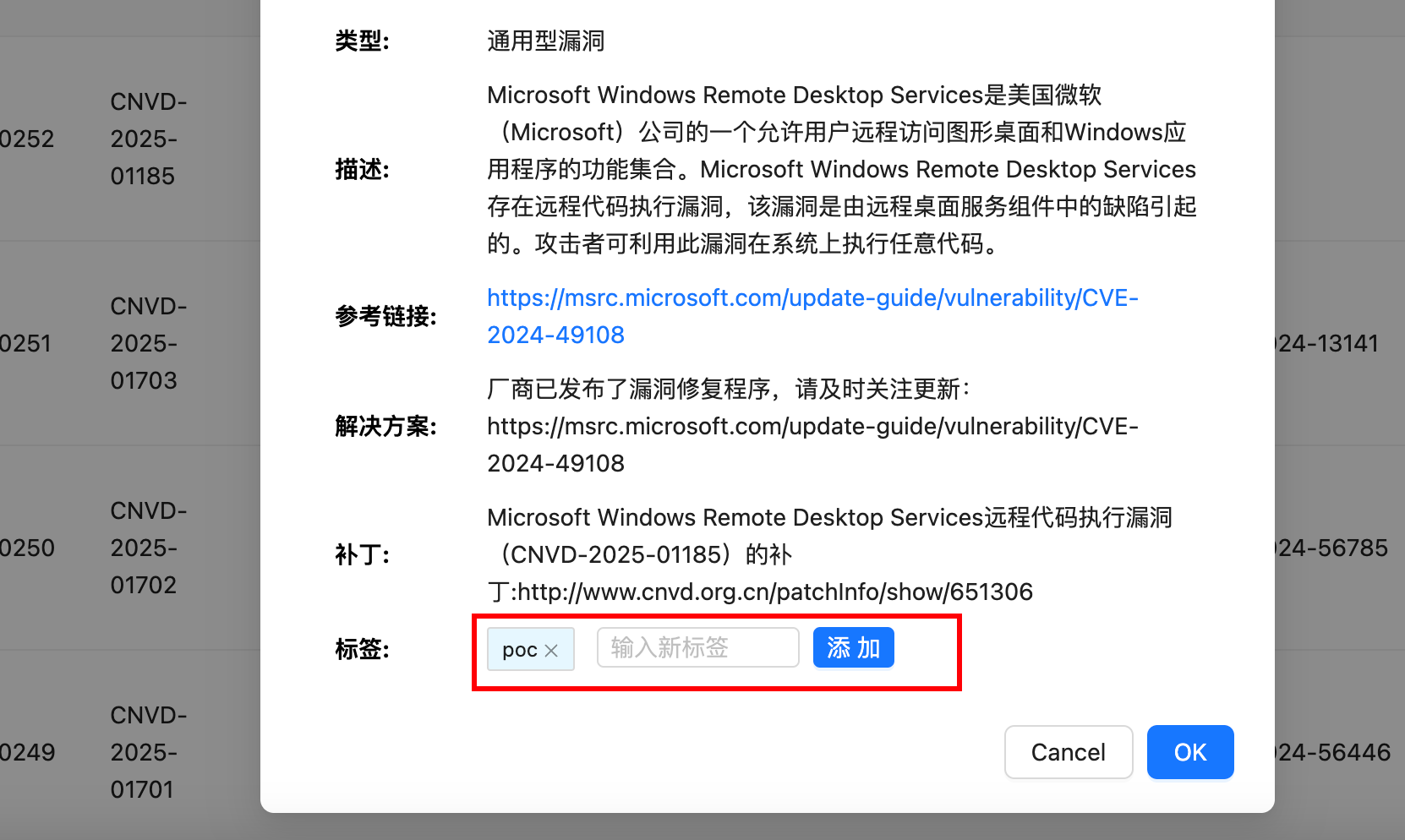
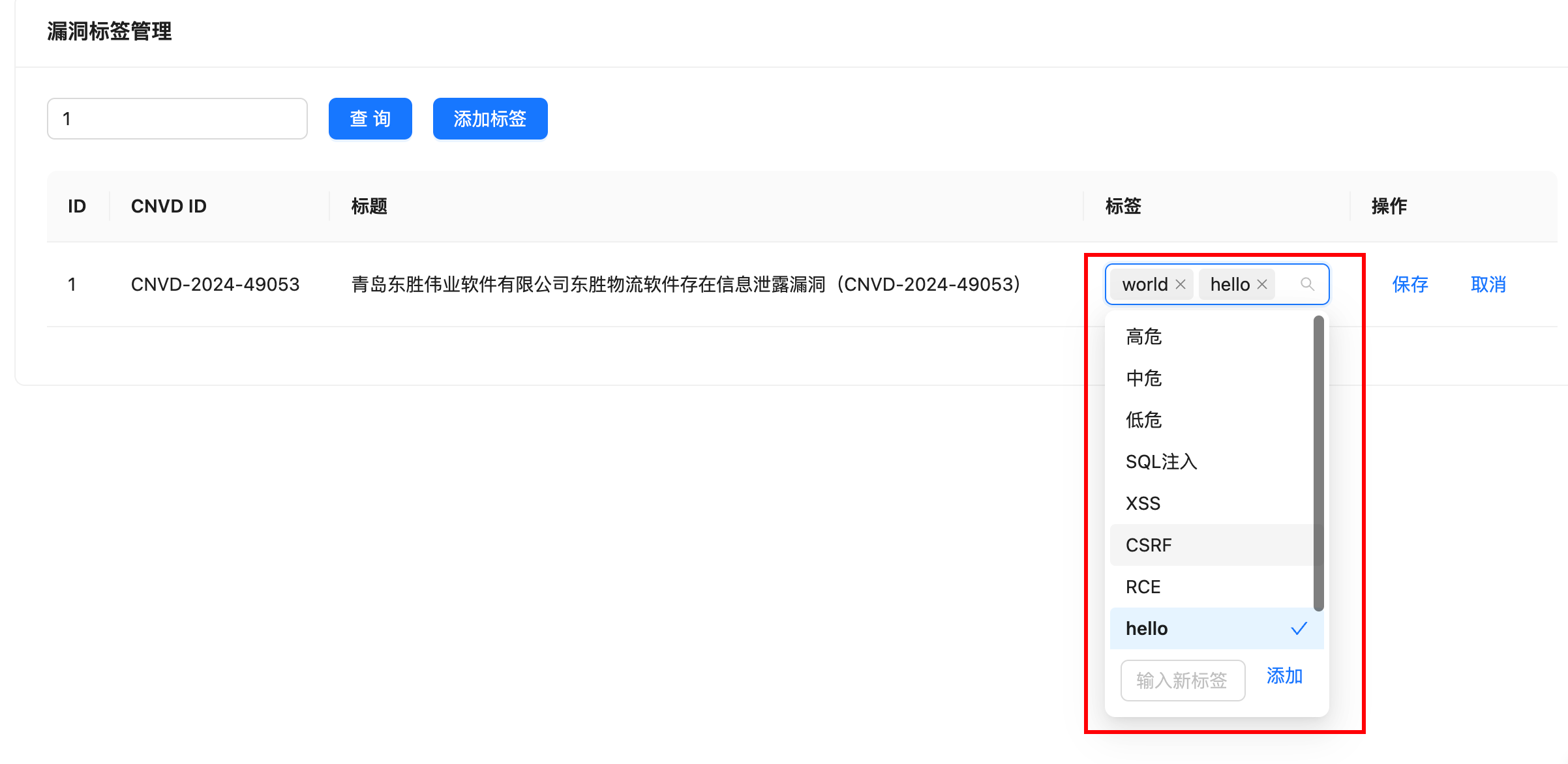
## 漏洞威胁情报 - 陈宇航、赵映雅、杨启程

**新增功能**

在“数据查询”页面新增自定义标签的添加和删除，点击 OK 按钮后向后端发送请求写库。

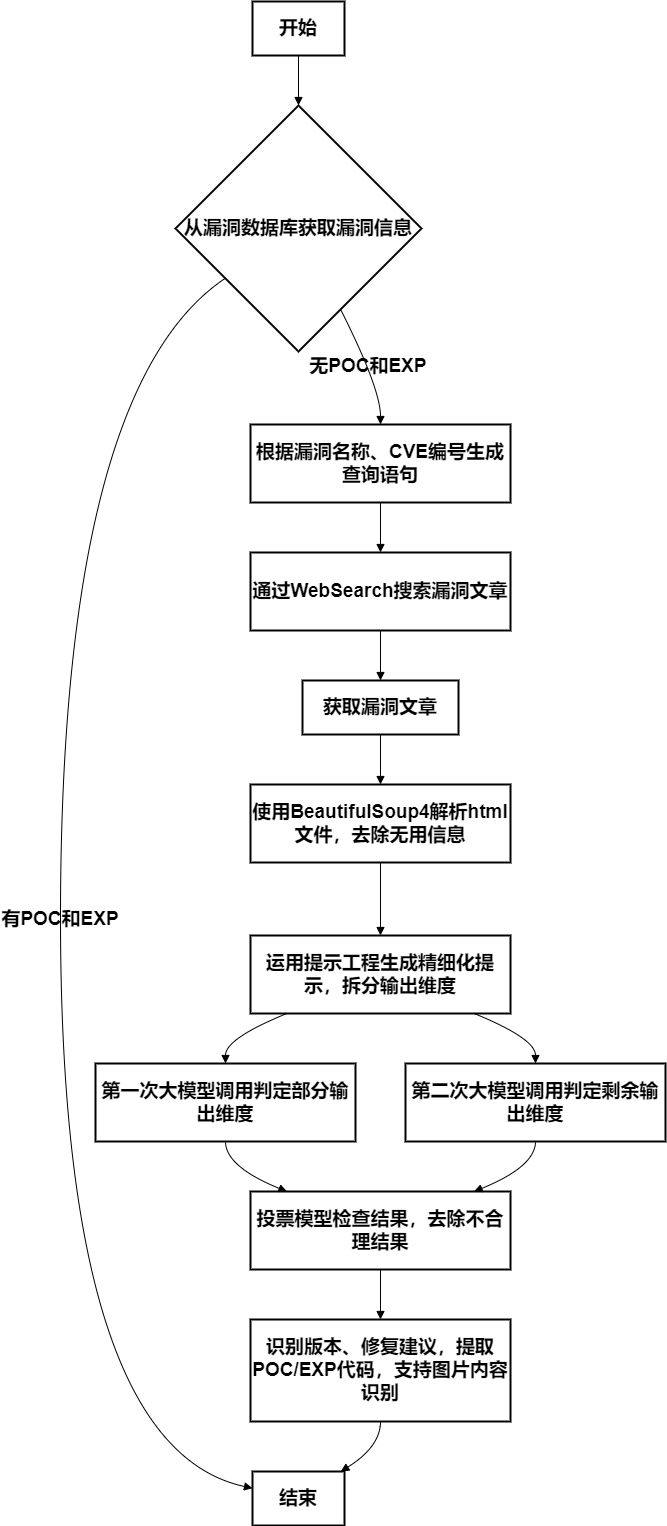


在“漏洞标签管理”页面新增自定义标签和预定义标签的添加删除，点击“保存”按钮后向后端发送请求写库。

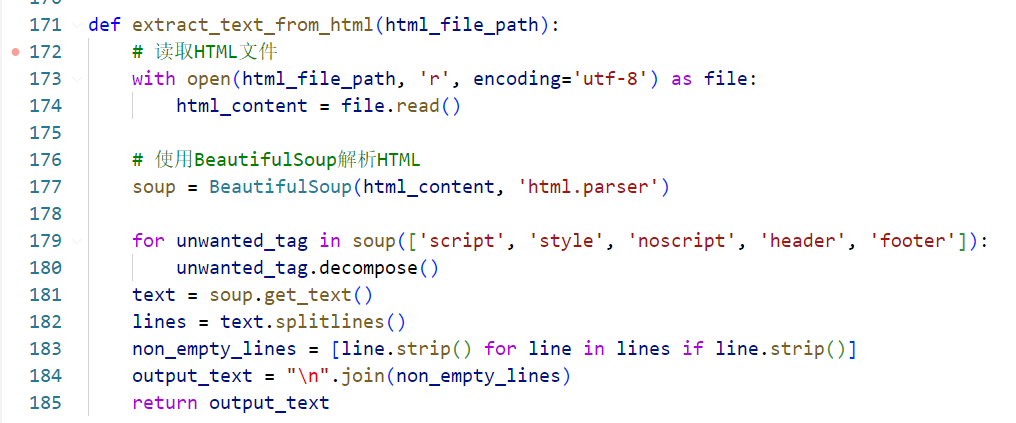


**新增需求点**

1. 在研究过程中发现，漏洞的文字描述等相关信息在数据库中有大量的保存，但是对于漏洞利用的POC和EXP信息数量却只占了很小的比重，考虑到组里的程序，最后属于漏洞利用和漏洞攻击的拦截，相关的POC和EXP方式对于漏洞的利用的攻击和拦截具有至关重要的作用，故想研发一套POC和EXP信息获取的功能框架，用于提取目标的漏洞相关信息。
2. 整体的框架流程制定如下：



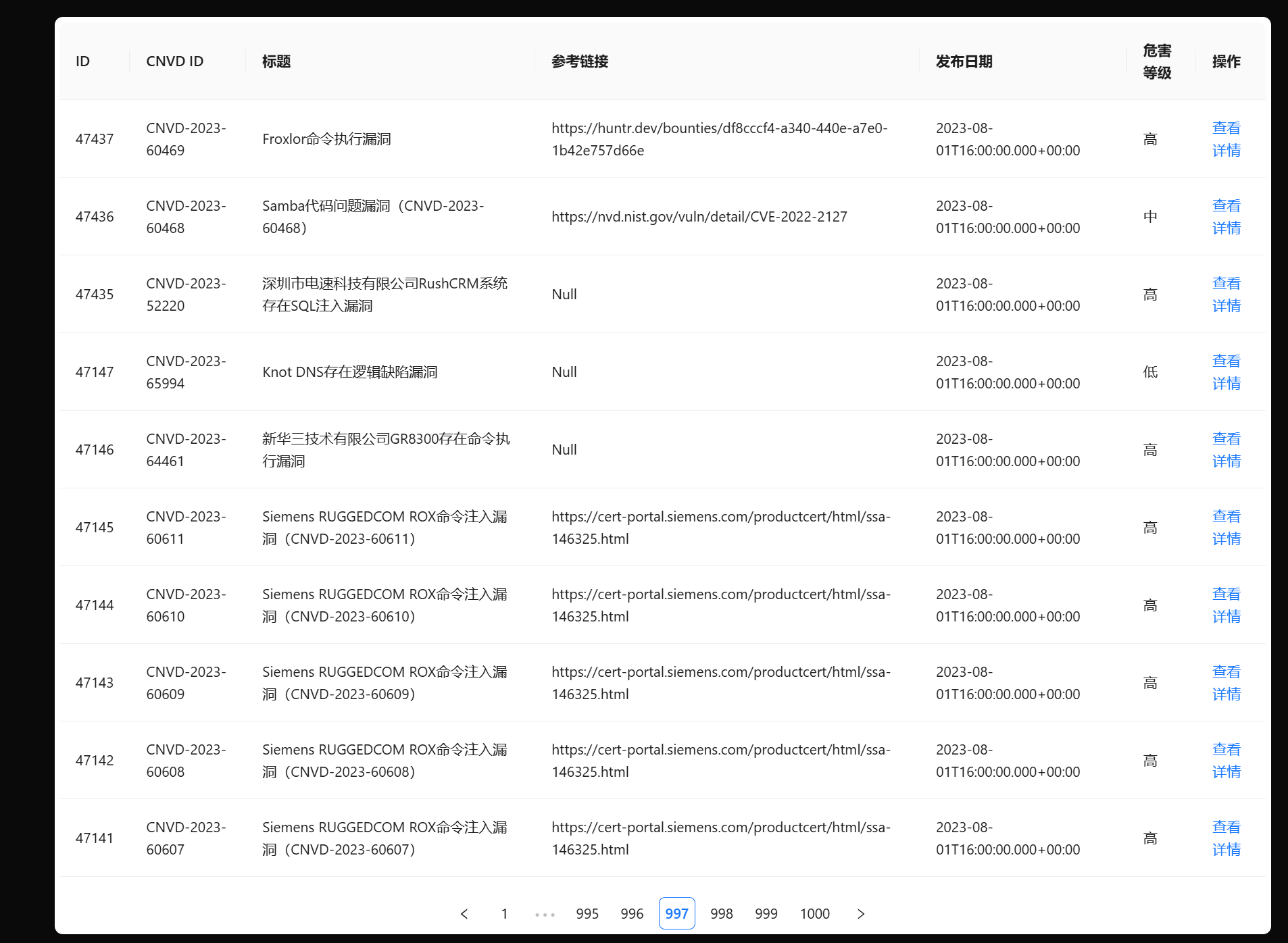
1. 主要功能点：
   1. 具备调用大模型 API 的能力，可对漏洞文章内的多维度信息实施自动批量化提取。待提取的信息维度涵盖文件名、漏洞编号、厂商或产品名称、编程语言、是否存在漏洞成因分析、危险函数名称、是否包含 POC/EXP 以及是否有 POC/EXP 解释。
   2. 在完成上述功能 1 的基础上，进一步对文章里的潜在 POC/EXP 进行判定并提取
   3. 能够对漏洞文章中的图片信息进行识别与提取
2. 目前代码功能模块正在开发：
   1. 采用langchain架构对接当前的免费智谱免费API用于对文章的多维度信息实施自动化的提取
   2. 代码开发示意图



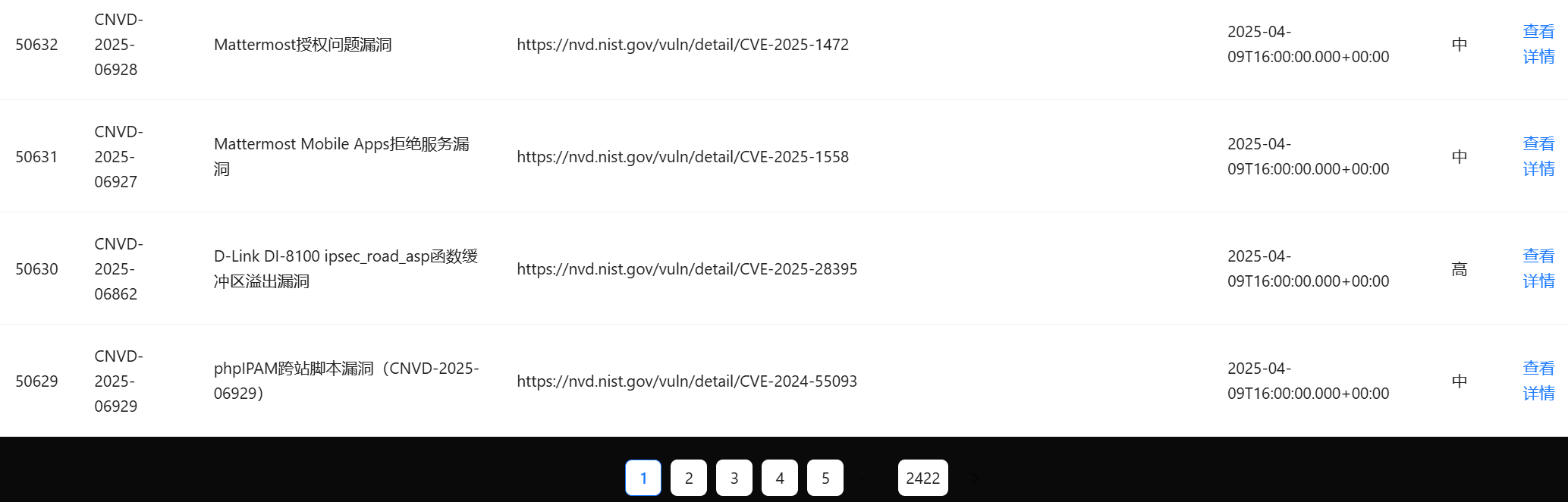
**前后端交互模块测试：**

数据库漏洞总量：24000+

最新1w条：



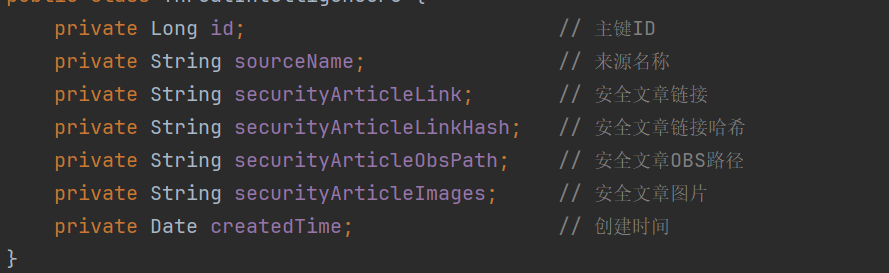
查询页面-无查询参数，显示全部：

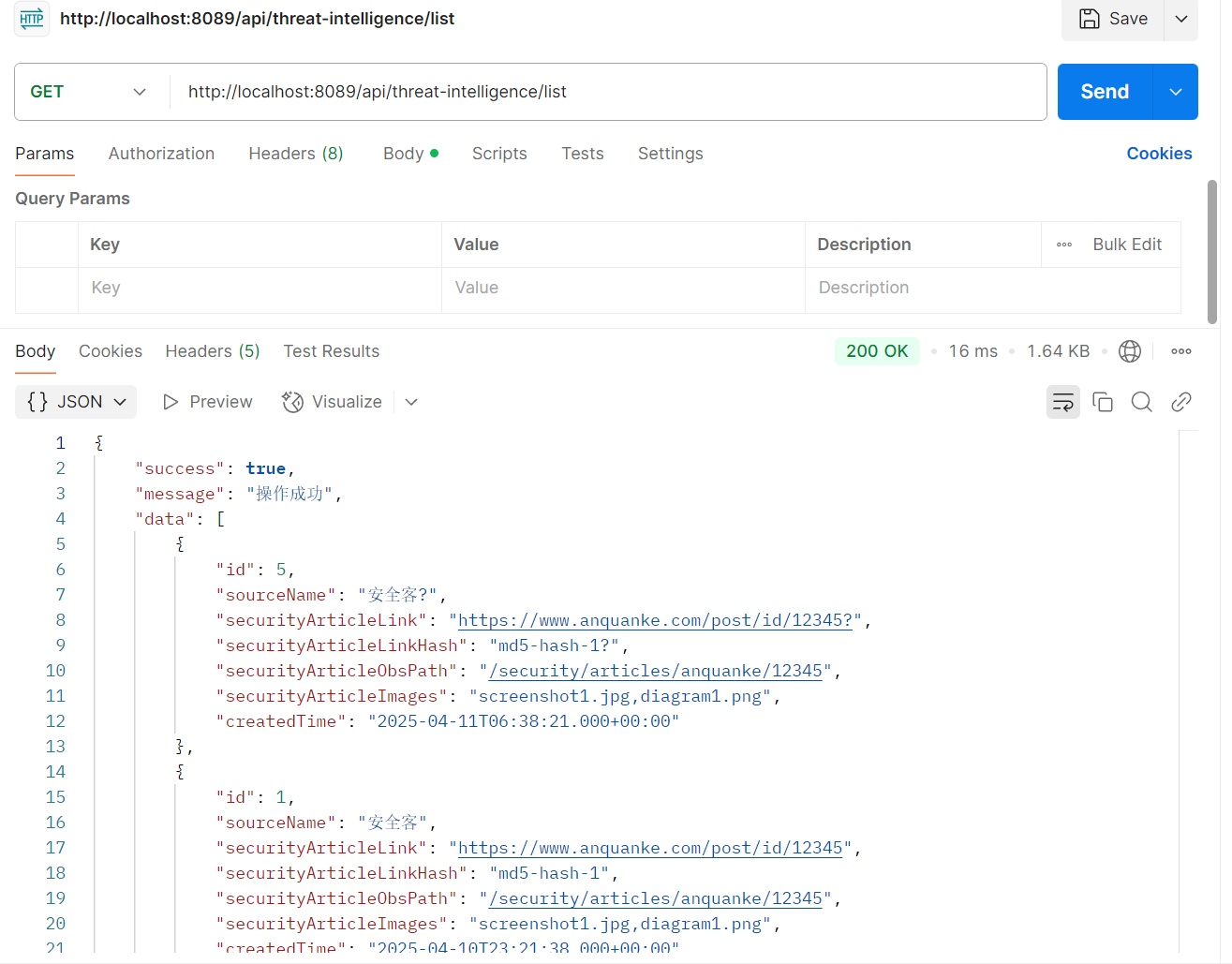


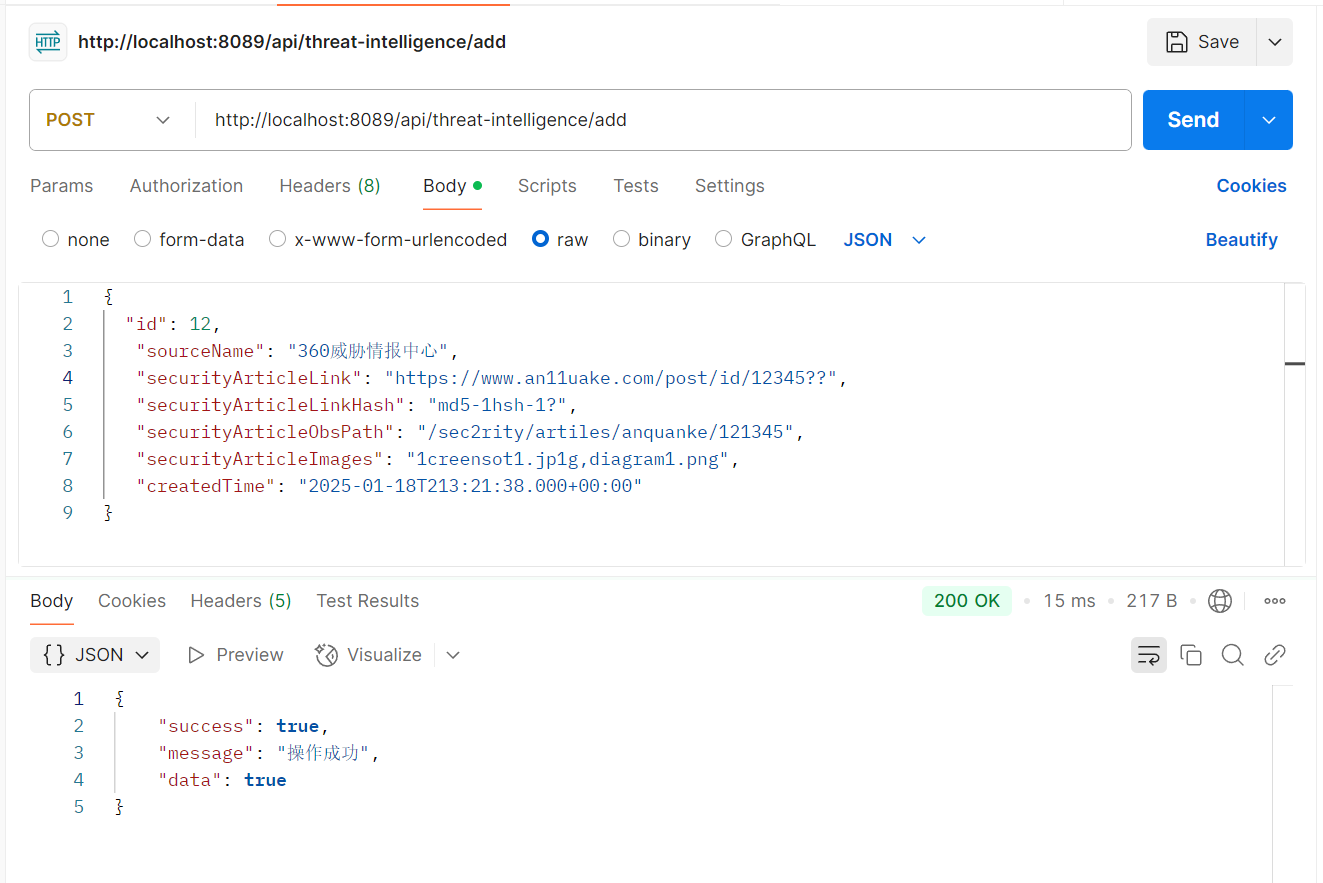
马嘉润、曾家豪、冯世玲 —— 威胁情报采集系统测试以及后端搭建

1. 对采集系统bug的修复，目前提高了webdriver的响应时间到30s，暂时没出现之前超时的问题，现在采集系统可以正常全量爬以及每日更新。
2. 威胁情报采集系统的后端搭建，设计了5个接口：添加威胁情报，根据ID查询，根据威胁情报来源查询，根据哈希查询，全量数据查询。

威胁情报包含以下核心字段：







1. 前端展示页面编写

